



**DEPARTMENT OF THE NAVY
HEADQUARTERS UNITED STATES MARINE CORPS
2 NAVY ANNEX
WASHINGTON, DC 20380-1775**

MCO 5238.2
LPS
11 Dec 96

MARINE CORPS ORDER 5238.2 W/CH 1-2

From: Commandant of the Marine Corps
To: Distribution List

Subj: Defense Automation Resources Management Program (DARMP)

Ref: (a) ASD C3I memo of 8 Sep 94 (NOTAL)
(b) SECNAVINST 5238.1C (NOTAL)

Encl: (1) System Authorization Access Request (SAAR)

1. Purpose. To publish policy and assign responsibility for the accounting and disposition of all automation resources (AR) within the Marine Corps.

2. Background. Reference (a) provides interim management guidance on the DARMP pending a revamp of DoD policy directives in the 8000 series regulations and reference (b). Marine Corps data stored in the Defense Information Technology Management System (DITMS) is used to develop acquisition and support strategies.

3. Action

a. The CMC (LPS) will:

(1) Serve as Marine Corps focal point for the DARMP.

(2) Review, validate, and maintain DITMS user access file.

(3) Support Marine Corps activities use of DITMS to maintain current inventory of AR and report excess AR via on-line or batch processing.

(4) Ensure the DoD Activity Address Code (DoDAAC) is tied to a Data Processing Installation (DPI) or Defense Reporting Activity (DRA) number.

(5) Attend DARMP focal point meetings to ensure consistency and compatibility throughout the entire DoD AR management program.

DISTRIBUTION STATEMENT A: Approved for public release;
distribution is unlimited.

MCO 5238.2
11 Dec 96

(6) Ensure that the Marine Corps activities comply with reference (a) and are provided interim management guidance on the subject program.

(7) Place available excess AR on hold major and subordinate commands.

(8) Review, validate, and forward DD Forms 122, 123 and 1149 used to redistribute AR to the Defense Information Systems Agency (DISA)/Chief Information Officer (DISA/CIO) for approval.

(9) Provide information on the various school donation programs.

(10) In coordination with the CMC (C4I), prepare the annual certification statement of the inventory of computer assets.

(11) Assist Marine Corps activities in resolving DITMS user problems.

b. The COMMARCORSYSCOM (CCR) will:

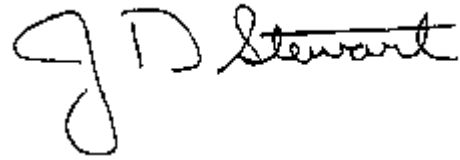
(1) Use Marine Corps data stored in DITMS as a single source tool to develop acquisition and support strategies announced via separate GENSER message data calls.

(2) Coordinate Integrated Logistics Support (ILS) and maintain the Marine Corps database for common computer resources to support use of the DARMP.

c. The COMMARFORLANT, COMMARFORPAC, COMMARFORRES, and Commanding Generals will:

(1) Established an AR control function within their organizational structure and at a minimum, designate a focal point for each major subordinate command (Div, Wing, FSSG, SRIG, MEF, and Base/Station/Post).

(2) Ensure that the enclosure is submitted to the CMC (LPS) for the responsible individual to obtain on-line access to the DARMP DITMS.



J. D. Stewart
Deputy Chief of Staff
for Installations and Logistics

DISTRIBUTION: PCN 10207717500

Copy to: 7000051 (100)
7000110 (55)
7000093/8145005 (2)
700099, 144/81445001 (1)

3



DEPARTMENT OF THE NAVY
HEADQUARTERS UNITED STATES MARINE CORPS
2 NAVY ANNEX
WASHINGTON, DC 20380-1775

MCO 5238.2 Ch 1
LPS
19 Aug 97

MARINE CORPS ORDER 5238.2 Ch 1

From: Commandant of the Marine Corps
To: Distribution List

Subj: DEFENSE AUTOMATION RESOURCES MANAGEMENT PROGRAM (DARMP)

Encl: (1) New page inserts to MCO 5238.2

1. Purpose. To transmit new page inserts and direct pen changes to the basis Order.

2. Action

a. Remove enclosure (1) of the basic Order and replace with enclosure (1) contain in the enclosure.

b. On the Promulgation page change enclosure to read "System Authorization Access Request (SAAR)."

c. In paragraph 3a(10), remove the word "mainframe" and replace with "the inventory of".

3. Change Notation. Paragraphs denoted by an asterisk (*) symbol contain changes not previously published.

4. Filing Instructions. File this Change transmittal immediately behind the signature page of the basic Order.



J. A. BURT
Assistant Deputy Chief of Staff
for Installations and Logistics

DISTRIBUTION: PCN 10207717501

Copy to: 7000051 (100)
7000110 (55)
7000093/8145005 (2)
7000099, 144/8145001 (1)

DISTRIBUTION STATEMENT A: Approved for public release;
distribution is unlimited.



**DEPARTMENT OF THE NAVY
HEADQUARTERS UNITED STATES MARINE CORPS
2 NAVY ANNEX
WASHINGTON, DC 20380-1775**

MCO 5238.2 Ch 2
LPS
21 Sep 98

MARINE CORPS ORDER 5238.2 Ch 2

From: Commandant of the Marine Corps
To: Distribution List

Subj: DEFENSE AUTOMATION RESOURCES MANAGEMENT PROGRAM (DARMP)

1. Purpose. To direct pen changes to the basic Order.

2. Action

a. In paragraph 2, remove the words "Automation Resources Management System (ARMS)" and replace with "Defense Information Technology Management System (DITMS)."

b. Replace the acronym "ARMS" with "DITMS" in paragraphs 3a(2), (3), and (11); 3b(1); and 3c(2).

c. Replace paragraph 3a(8) with the following paragraph
"Review, validate, and forward DD Forms 122, 123 and 1149 used to redistribute AR to the Defense Information System Agency (DISA)/Chief Information Officer (DISA/CIO) for approval."

d. In enclosure (1), page 2, line 14, remove the words "Automation Resources Management System (ARMS)" and replace with "Defense Information Technology Management System (DITMS)."

3. Filing Instructions. This Change transmittal will be filed immediately following page 5 of the basic Order.

A handwritten signature in dark ink, appearing to read "G. B. Higginbotham", is located in the lower right quadrant of the page.

G. B. HIGGINBOTHAM
Deputy Chief of Staff

for Installations and Logistics

DISTRIBUTION: PCN 10207717502

Copy to: 7000051 (100)
7000110 (55)
7000093/8145005 (2)
7000099, 144/8145001 (1)

7

MCO 5238.2 Ch 1
11 Dec 96

MCO 5238.2 Ch 1
11 Dec 96

SYSTEM AUTHORIZATION ACCESS REQUEST (SAAR)

SYSTEM AUTHORIZATION ACCESS REQUEST (SAAR)			
PRIVACY ACT STATEMENT			
Public Law 99-474, the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, authorizes collection of this information. The information will be used to verify that you are an authorized user of a Government automated information system (AIS) and/or to verify your level of Government security clearance. Although disclosure of the information is voluntary, failure to provide the information may impede or prevent the processing of your "System Authorization Access Request (SARR)". Disclosure of records or the information contained therein may be specifically disclosed outside the DoD according to the "Blanket Routine Uses" set for at the beginning of the DISA compilation of systems of records, published annually in the Federal Register, and the disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act.			
TYPE OF REQUEST	<input type="checkbox"/> INITIAL	<input type="checkbox"/> MODIFICATION	<input type="checkbox"/> DELETION
			DATE
PART I (To be completed by User)			
1. NAME (LAST, First, MI)		2. SOCIAL SECURITY NUMBER	
3. ORGANIZATION	4. OFFICE SYMBOL/DEPARTMENT		5. ACCOUNT CODE
6. JOB TITLE/FUNCTION		7. GRADE/RANK	8. PHONE (DSN)
STATEMENT OF ACCOUNTABILITY			
I understand my obligation to protect my password. I assume the responsibility for data and system I am granted access to. I will not exceed my authorized access.			
USER SIGNATURE			DATE
PART II (To be completed by User's Security Manager)			
9. CLEARANCE LEVEL	10. TYPE OF INVESTIGATION		11. DATE OF INVESTIGATION
12. VERIFIED BY (Signature)		13. PHONE NUMBER	14. DATE
PART III (To be completed by User's Supervisor)			
15. ACCESS REQUIRED (Location) - i.e. DMC or DMC's			
16. ACCESS TO CLASSIFIED REQUIRED?		17. TYPE OF USER	
<input type="checkbox"/> NO <input type="checkbox"/> YES		<input type="checkbox"/> FUNCTIONAL <input type="checkbox"/> SYSTEM	
		SECURITY ADMINISTRATOR APPLICATION DEVELOPER OTHER (Specify)	
18. JUSTIFICATION FOR ACCESS			
VERIFICATION OF NEED TO KNOW			
I certify that this user requires access as requested in the performance of his/her job function.			
19. SIGNATURE OF SUPERVISOR		20. ORG./DEPT.	21. PHONE NUMBER
			22. DATE
23. SIGNATURE OF FUNCTIONAL DATA OWNER/OPR		24. ORG./DEPT.	25. PHONE NUMBER
			26. DATE
PART IV (To be completed by AIS Security Staff adding user)			
27. USERID (Mainframe)		28. USERID (Mid-Tier)	
		29. USERID (NetWork)	
30. SIGNATURE		31. PHONE NUMBER	32. DATE

DISA Form 41, SEP 1996 (EF)

DISA FORM 41, SEP 1996 (EF)
Form 41, SEP 1996 (EF)

ENCLOSURE (1)
Ch 1 (19 Aug 97)

ENCLOSURE (1)
Ch 1 (19 Aug 97)

MCO 5238.2 Ch 1
11 Dec 96

ENCLOSURE (1)

MCO 5238.2 Ch 1
11 Dec 96

DEPARTMENT OF DEFENSE
DEFENSE INFORMATION SYSTEMS AGENCY (DISA)
CHIEF INFORMATION OFFICER
DEFENSE AUTOMATION RESOURCES MANAGEMENT PROGRAM DIVISION
SYSTEM ACCESS AUTHORIZATION REQUEST
PART V

DPI Code: _____ DODAAC: _____
Directorate/Division: _____
Attention: _____
Street/Box #: _____
City - State: _____ Fax: _____
Zip: _____ E-mail Address: _____

Automation Resources Management System (ARMS) Users Access:

- a. Select One or More:
☐ Active Hardware Inventory
☐ Redistribution/Excess Hardware Inventory
- b. Select One:
☐ Read Only
☐ Read/Update

If "Read/Update" is selected, list Defense Reporting
Activities (DRA's) you will update:

Obtain DARMP Focal Point Signature
(Ref: www.disa.cio/darmp Web Page, Focal Point List)

Signature: _____

Agency: _____ Date: _____

Applicant's Major Command(Office Code): _____

Procedures: When you have completed both pages of the System Authorization Access Request (SAAR), please fax to your DARMP Focal Point for approval. Your DARMP Focal Point will pass the SAAR to the DARMP Division for processing. Contact the DARMP Division on (703) 696-1904 or DSN 426 if you are unable to locate information pertaining to your DARMP Focal Point.

ENCLOSURE (1)
Ch 1 (19 Aug 97)

MCO 5238.2 CH 1
11 Dec 96

MCO 5238.2 Ch 1
11 Dec 96

INSTRUCTIONS

A. PART I: The following information is provided by the user when establishing or modifying their USERID.

- (1) NAME: The last name, first name, and middle initial of the user.
 - (2) SOCIAL SECURITY NUMBER: The social security number of user.
 - (3) ORGANIZATION: The user's current organization (*i.e.*, DMC Columbus).
 - (4) OFFICE SYMBOL/DEPARTMENT: The office symbol within the current organization (*i.e.*, WEC03).
 - (5) ACCOUNT CODE: Account code, if required.
 - (6) JOB TITLE/FUNCTION: The job function (*i.e.*, System Analyst, Pay Clerk, etc.).
 - (7) GRADE/RANK: The civilian pay grade, military rank or CONT if user is a contractor.
 - (8) PHONE (DSN): The Defense Switching Network (DSN) phone number of the user. If DSN is unavailable, indicate commercial number.
- USER'S SIGNATURE: User must sign the SAAR form with the understanding that they are responsible and accountable for their password and access to the system(s).

B. PART II: The following information is provided by the User's Security Manager.

- (9) CLEARANCE LEVEL: The user's current security clearance level and ADP Level (*i.e.*, Secret, Top Secret, ADP I, ADP III, etc.).
- (10) TYPE OF INVESTIGATION: The user's last type of background investigation. (*i.e.*, NAC, NACI, or SSB).
- (11) DATE OF INVESTIGATION: The date of the last background investigation.
- (12) SIGNATURE: The Security Manager or his representative signature indicates that the above clearance and investigation information has been verified.
- (13) PHONE NBR: The Security Manager's phone number.
- (14) DATE: The date that the form was signed by the security manager or his representative.

C. PART III: The following information is provided by the user's supervisor.

- (15) ACCESS REQUIRED (Location): The full name of the location at which access is required.
- (16) ACCESS TO CLASSIFIED REQUIRED?: Place an "X" in the appropriate box.
- (17) TYPE OF USER: Place an "X" in the appropriate box.
- (18) JUSTIFICATION FOR ACCESS: A brief statement to justify establishment of an initial USERID. Provide appropriate information if the USERID or access to the current USERID is to be modified.
- (19) SIGNATURE OF SUPERVISOR: The user's supervisor must sign the SAAR form to certify the user is authorized access to perform his/her job function.
- (20) ORG./DEPT.: Supervisor's organization and department.
- (21) PHONE NUMBER: Supervisor's phone number.
- (22) DATE: The date the supervisor signs the SAAR form.
- (23) SIGNATURE OF FUNCTIONAL DATA OWNER/OPR: Signature of the functional appointee responsible for approving access to the system being requested.
- (24) ORG./DEPT.: Functional appointee's organization and department.
- (25) PHONE NUMBER: Functional appointee's phone number.
- (26) DATE: The date the Functional appointee signs the SAAR form.

D. PART IV: The following information is provided by the AIS Security Staff who adds the user to the system.

- (27) USERID (Mainframe): User's mainframe USERID (*if applicable*).
- (28) USERID (Mid-Tier): User's mid-tier USERID (*if applicable*).
- (29) USERID (Network): User's network USERID (*if applicable*).
- (30) SIGNATURE: Signature of the Information System Security Officer (ISSO) or his representative.
- (31) PHONE NUMBER (DSN): The ISSO's Defense Switching Network (DSN) phone number.
- (32) DATE: The date the ISSO signs the SAAR form.

E. PART V: This information is site specific and can be customized by either the DMC, functional activity, or the customer with approval of the DMC. This information will specifically identify the access required by the user.

- (33) ACCESSES REQUIRED: Specify all resources to which access is required and the type of access required. *i.e.*, read-only, write.
- (34) OPTIONAL USE: This section is intended to add site specific information, as required.

F. DISPOSITION OF FORM:

TRANSMISSION: Form may be electronically transmitted, faxed, or mailed. Adding a password to this form makes it a minimum of "FOR OFFICIAL USE ONLY" and must be handled as such.

FILING: Original SAAR, with original signatures in Parts I, II, and III, must be maintained on file for one year after termination of user's account. File may be maintained by the DMC or by the Customer's ISSO. Recommend file be maintained by ISSO adding the user to the system.

DISA Form 41, SEP 1996 (EF)

DISA (R) IDTS, Inc.
FormFlow V1.00

ENCLOSURE (1)
Ch 1 (19 Aug 97)